

How We Absorbed 748 Gbps DDoS Attack Without Missing a Beat



A few days ago, our monitoring tools lit up. Our network caught a **748 Gbps volumetric DDoS attack** — a flood of malicious traffic designed to choke our pipes, knock servers offline, and bring client sites to a dead stop.

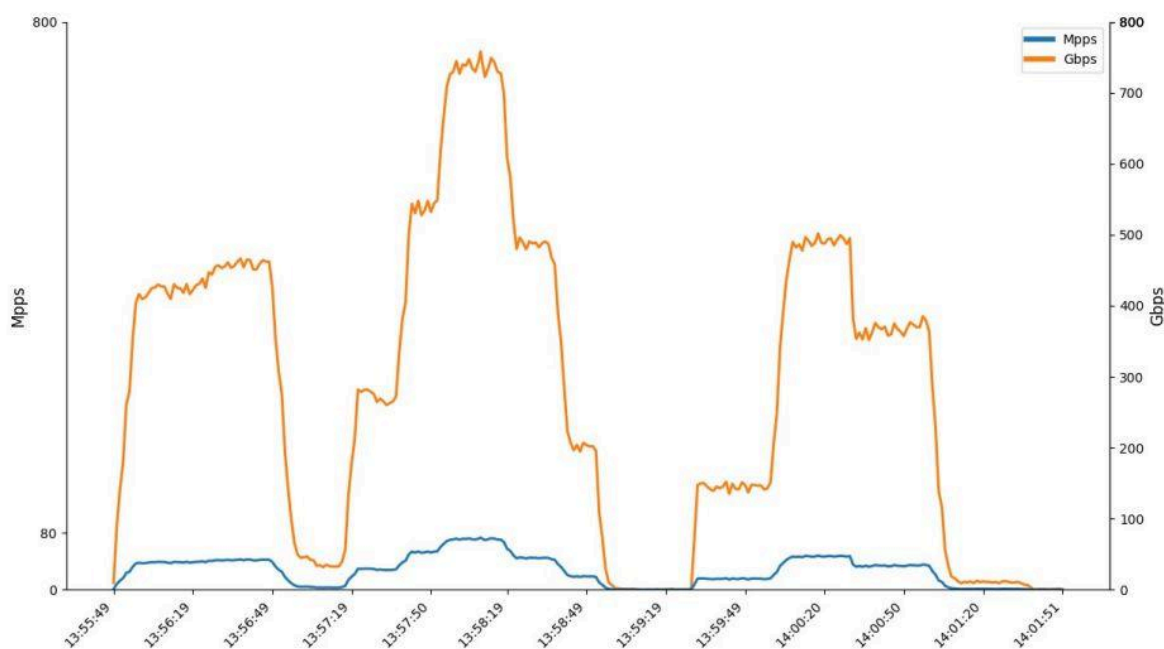
If your server is hosted with us, you probably didn't notice a thing. Your site stayed online, response times didn't spike, and nothing changed on your end.

Here's what happened behind the scenes, and how our DDoS protection handled it.

What a 748 Gbps DDoS Attack Actually Looks Like

748 Gbps isn't a traffic spike it's an aggressive, full-scale volumetric attack. Instead of trying to hack into an app or breach a database, the attacker simply dumps enough junk data at our doorstep to plug the entire line.

This one was a multi-vector attack, mixing high-rate SYN floods with UDP amplification, aimed at overwhelming our edge routers before we could react.



- **Gbps Peak (Orange line):** Touches just under **748 Gbps**.
- **Mpps Peak (Blue line):** Peaks around **80–90 Mpps** (Million Packets Per Second).

That's the scale of attack most "free DDoS protection" hosting plans are never actually tested against.

The Dirty Secret of Budget DDoS Protection

Almost every hosting company advertises "free enterprise DDoS protection." But when a real, large-scale attack hits, here's what usually happens behind closed doors.

They blackhole (null-route) your IP.

When a 500+ Gbps attack hits a standard host, their team realizes filtering it costs more bandwidth and processing power than they've budgeted for. So they take the easy way out: they switch off your server's IP address.

The attacker gets exactly what they wanted your server is down, your site is invisible, and your customers assume you've disappeared.

To us, killing a client's IP to "protect" it isn't protection it's surrender to attacker.

How Our [DDoS Protection](#) Actually Mitigated This

No null-routes, no downtime, no manual intervention at 2 AM. This is engineered network defense, not a third-party CDN shield:

- **BGP-based traffic engineering**, run on our own autonomous system (AS151704), let us steer and control routing paths in real time instead of depending on someone else's network
- **On-prem hardware and appliance-based filtering** sat at the edge, dropping malicious packets before they ever touched client servers
- **In-house custom filtering** firewall rules and rate-limiting tuned to this attack's signature separated the SYN flood and UDP amplification traffic from legitimate connections without collateral damage

Client-facing result: uptime held, latency held, and nobody had to file a support ticket.

Why We Care So Much About Infrastructure

Behind every website, app, or database we host, there's a business owner who worked hard to earn their traffic. When an attacker takes aim at your server, they're not just sending bad packets they're attacking your revenue, your search rankings, and your reputation.

We build, tune, and stress-test our infrastructure specifically so you don't wake up to a panicked message that your site is down. You focus on growing the business. We keep the pipes clean.

Is Your Current Provider Ready for a 700+ Gbps Surge?

If you've dealt with downtime, surprise null-routes, or slow support when things break, it may be time to [move to our cloud](#) actually built for modern DDoS threats.